

## CLAIMS

What is claimed is:

- 1    1. A method for authenticating messages communicated between partners that belong to  
2       a plurality of partners, the method comprising the steps of:  
3           maintaining at a trusted intermediary a signature decryption key for each partner of  
4           said plurality of partners that is authorized to use said trusted intermediary to  
5           send messages;  
6           receiving at said trusted intermediary messages originated by partners of said plurality  
7           of partners that are intended for other partners of said plurality of partners;  
8           for each message thus received, the trusted intermediary performing the steps of  
9           using the signature decryption key associated with the partner that sent the  
10          message to determine whether the message was actually sent by that  
11          partner; and  
12          if the message was actually sent by that partner, then sending the message to  
13          the partner for which the message is intended along with a digital  
14          signature of said trusted intermediary to indicate that the trusted  
15          intermediary has verified that the message was actually sent by the  
16          partner that sent the message.
  
- 1    2. The method of Claim 1 wherein the signature decryption key for each partner of said  
2       plurality of partners is a public signature decryption key associated with a private  
3       signature creation key.

- 1       3. The method of Claim 1 wherein the signature decryption key for each partner of said  
2                  plurality of partner is used to decrypt a digital signature associated with a message  
3                  that is sent along with the digital signature.
- 1       4. The method of Claim 1 wherein the digital signature of the trusted intermediary is  
2                  associated with a message that is sent along the digital signature of the trusted  
3                  intermediary.
- 1       5. The method of Claim 1 wherein the digital signature of the trusted intermediary is  
2                  encrypted by a private signature creation key associated with a public signature  
3                  decryption key.
- 1       6. A computer-readable medium storing computer code for causing a computer to  
2                  perform a method for authenticating messages communicated between partners that  
3                  belong to a plurality of partners, by the steps of:  
4                                  maintaining at a trusted intermediary a signature decryption key for each  
5                                  partner of said plurality of partners;  
6                                  receiving at said trusted intermediary messages originated by partners of said  
7                                  plurality of partners that are intended for other partners of said  
8                                  plurality of partners;  
9                                  for each message thus received, the trusted intermediary performing the steps  
10                                  of

11                   using the signature decryption key associated with the partner that sent  
12                   the message to determine whether the message was actually  
13                   sent by that partner; and  
14                   if the message was actually sent by that partner, then sending the  
15                   message to the partner for which the message is intended along  
16                   with a digital signature of said trusted intermediary to indicate  
17                   that the trusted intermediary has verified that the message was  
18                   sent actually sent by the partner that sent the message.

- 1     7.   The computer-readable medium of Claim 6 wherein the signature decryption key for  
2       each partner is a public signature decryption key associated with a private signature  
3       creation key.
- 1     8.   The computer-readable medium of Claim 6 wherein the signature decryption key for  
2       each partner is used to decrypt a digital signature associated with a message is that  
3       sent along with the digital signature.
- 1     9.   The computer-readable medium of Claim 6 wherein the digital signature of the trusted  
2       intermediary is associated with a message that is sent along with the digital signature.
- 1     10.   The computer-readable medium of Claim 6 wherein the digital signature of the trusted  
2       intermediary is encrypted by a private signature creation key associated with a public  
3       signature decryption key.

storage means configured to store a signature decryption key for each partner of said plurality of partners that is authorized to use said computer to send messages;

receiving means configured to receive messages that are originated by partners of said plurality of partners and that are intended for other partners of said plurality of partners;

signature decryption means; and

sending means; wherein

for each message thus received,

said signature decryption means is configured to use the signature

decryption key associated with the partner that sent the

message to determine whether the message was actually sent

by that partner; and

if the message was actually sent by that partner, said sending means is

configured to send the message along with a digital signature

of said trusted intermediary to the partner for which the

message is intended; wherein said digital signature of said

trusted intermediary is used to indicate that said trusted

intermediary has verified that the message was actually sent.

the partner that sent the message.

1       12. The computer of claim 11 further comprising signature encryption means by which  
2                   said digital signature of said trusted intermediary was created.

1       13. A computer network for use in communications between partners that belong to a  
2                   plurality of partners, comprising:

3                   a plurality of computers each of which is configured to store a respective  
4                   signature creation key of a partner of said plurality of partners that is  
5                   authorized to use a trusted intermediary computer to send messages;

6                   wherein said trusted intermediary computer is configured  
7                   to store a plurality of signature decryption keys each of which  
8                   corresponds to the respective signature creation key that is  
9                   stored in each of said plurality of computers;

10                  wherein, upon receiving messages that are originated by partners of said  
11                  plurality of partners and that are intended for other partners of said  
12                  plurality of partners, said trusted intermediary computer, for each  
13                  message thus received, is configured

14                   to use the signature decryption key associated with the partner  
15                   that sent the message to determine whether the message  
16                   was actually sent by that partner; and

17                   if the message was actually sent by that partner, then sending  
18                   the message to the partner for which the message is  
19                   intended along with a digital signature of said trusted  
20                   intermediary to indicate that the trusted intermediary

21 has verified that the message was actually sent by that  
22 partner that sent the message.

1    15. The method of Claim 14 wherein the message encryption key for each partner of said  
2        plurality of partners is a public message encryption key associated with a private  
3        message decryption key.

3           partners was encrypted using a message encryption key associated with the trusted  
4           intermediary.

1       17. The method of Claim 16 wherein said message encryption key associated with said  
2           trusted intermediary is a public message encryption key that is associated with a  
3           private message decryption key.

1       18. A computer-readable medium storing computer code for causing a computer to  
2           perform a method for a trusted intermediary to manage keys used in communications  
3           between partners that belong to a plurality of partners, by the steps of:

4                   said trusted intermediary maintaining a message encryption key for each  
5                   partner of said plurality of partners that is authorized to use said  
6                   trusted intermediary to receive messages; wherein  
7                   upon receiving messages originated by partners of said plurality of partners  
8                   that are intended for other partners of said plurality of partners, said  
9                   trusted intermediary, for each message thus received, performing the  
10                  steps of

11                   encrypting the message using the message encryption key  
12                   associated with the partner for which the message is  
13                   intended; and

14                   sending the encrypted message to the partner for which the  
15                   message is intended.

1    19. The computer-readable medium of Claim 18 wherein the message encryption key for  
2        each partner of said plurality of partners is a public message encryption key  
3        associated with a private message decryption key.

1    20. The computer-readable medium of Claim 18 wherein the computer further performs  
2        the step of:

3                each partner of said plurality of partners that sends messages to said trusted  
4        intermediary maintains a message encryption key associated with a  
5        message decryption key of said trusted intermediary.

1    21. The computer-readable medium of Claim 20 wherein said message encryption key  
2        associated with said message decryption key of said trusted intermediary is a public  
3        message encryption key and said message decryption key of said trusted intermediary  
4        is a private message decryption key.

1    22. A computer for use in communications between partners that belong to a plurality of  
2        partners, comprising:

3                storage means configured to store a message encryption key for each partner  
4        of said plurality of partners that is authorized to use said computer to  
5        receive messages;

6                message encryption means;

7                sending means; and

8 receiving means configured to receive messages that are originated by  
9 partners of said plurality of partners and that are intended for other  
10 partners of said plurality of partners; wherein  
11 for each message thus received,  
12 said message encryption means encrypts the message using the  
13 message encryption key associated with the partner for which  
14 the message is intended; and  
15 said sending means sends the encrypted message to the partner for  
16 which the message is intended.

1 23. The computer system of claim 22 further comprising message decryption means that,  
2 for each message thus received, produces that message from an encrypted message.

1 24. A computer network for use in communications between partners that belong to a  
2 plurality of partners, comprising:  
3 a plurality of computers each of which is configured to store a respective  
4 message decryption key of a partner of said plurality of partners that is  
5 authorized to use a trusted intermediary computer to receive messages;  
6 wherein said trusted intermediary computer is configured  
7 to store a plurality of message encryption keys each of which  
8 corresponds to the respective message decryption key that is  
9 stored in each of said plurality of computers;  
10 wherein, upon receiving messages that are originated by partners of said  
11 plurality of partners and that are intended for others partners of said

12                   plurality of partners, said trusted intermediary computer, for each  
13                   message thus received, is configured  
14                   to encrypt the message using the message encryption key  
15                   associated with the partner for which the message is  
16                   intended, and  
17                   to send the encrypted message to the partner for which the  
18                   message is intended.